

## REMARKS

### **I. General**

Claims 1-39 were pending in the present application and were rejected in the current Office Action (mailed May 7, 2004). The outstanding issues in the current Office Action are:

- Claims 1, 10, 11, 13-18, and 37 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,347,374 issued to Drake et al. (hereinafter “*Drake*”);
- Claims 2-9, 19-36, and 38-39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of U.S. Patent No. 5,920,719 issued to Sutton et al. (hereinafter “*Sutton*”); and
- Claim 12 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of U.S. Patent No. 6,253,337 issued to Maloney et al. (hereinafter “*Maloney*”).

In response, Applicant respectfully traverses the outstanding claim rejections, and requests reconsideration and withdrawal thereof in light of the amendments and remarks presented herein.

### **II. Amendments**

Claim 28 is amended and new claims 40-54 are added herein. No new matter is added by this amendment and newly presented claims.

Claim 28 is amended herein to recite “receiving input from a user” for creating the recited audit transformation template. This element is supported by, *inter alia*, the specification at page 12, lines 8-10.

Newly added claims 40-54 are supported by, *inter alia*, the specification at page 12, lines 10-15 and page 14, line 20 – page 15, line 11.

### **III. Rejections under 35 U.S.C. § 102(e) over *Drake***

Claims 1, 10, 11, 13-18, and 37 are rejected under 35 U.S.C. § 102(e) as being anticipated by *Drake*. Applicant respectfully traverses this rejection as provided further below.

To anticipate a claim under 35 U.S.C. § 102, a single reference must teach every element of the claim, *see* M.P.E.P. § 2131. Applicant respectfully submits that *Drake* fails to teach each and every element of claims 1, 10, 11, 13-18, and 37, as discussed below.

**A. Independent Claims 1, 14, and 37**

*Drake* fails to teach each of the elements of independent claims 1, 14, and 37. For instance, independent claim 1 recites in part “software code executable by at least one processor to receive said collected audit data and generate output comprising at least a portion of said collected audit data in a desired format defined by a template, wherein said desired format is different than said first format” (emphasis added).

Similarly, independent claim 14 recites in part “code executable to generate output comprising at least a portion of said collected audit data, said output having a format defined by said audit transformation template” (emphasis added).

Finally, independent claim 37 recites in part “function executable to generate output comprising at least a portion of said collected audit data, wherein said output has a format defined by said template” (emphasis added).

*Drake* fails to teach at least the above elements of these independent claims. *Drake* at col. 5, lines 21-32 provides an event detection system:

which can be viewed as a dual three-tiered implementation with a database 12 in the middle. On one side is an audit analysis engine 14, which converts raw audit data into a standardized format, and performs expert system analysis on the data. On the other side is a user interface 16, which consists of management and control functions, and an application user interface that provides data mining tools to the use of the invention referred to herein as the event detection system.

In *Drake*, events are:

stored in relational database 12 in a normalized format, i.e., standard, that maximizes storage capacity and flexibility. The normalized format also simplifies analysis of events, in that no matter what the audit source 18, the events are represented in a single format. Col. 5, lines 62-67.

External to the database 12, events are passed between processes in a standardized representation referred to as a Virtual Record. The Virtual Record is a standardized flat

representation of an event in normalized format. Col. 6, lines 4-8. “A parser 20 performs the audit parsing, and has as its sole function the conversion of raw event records into Virtual Records.” Col. 7, lines 37-39.

Accordingly, *Drake*’s event detection system standardizes audit data and stores the standardized audit data to a database, where a user interface can be used for querying the database. However, *Drake* does not teach that templates are used for transforming the audit data from its raw format to the standardized/normalized format. That is, *Drake* does not teach that the parser 20 uses templates for performing this transformation.

In asserting that *Drake* teaches this element of claim 1, the present Office Action cites to element 38 of FIG. 1 and col. 2, lines 45-55 of *Drake*. However, these cited portions of *Drake* make no mention of using a template for defining an output format. For instance, element 38 of FIG. 1 is taught as being a “sender”, and is not taught as using a template for defining an output format. Particularly, col. 10, lines 11-20 describe the sender 38 as follows:

The generic file transfer utilities 30, in one embodiment, include a sender 38 that provides an ability to automate periodic transfer of files over a distributed network, be they raw audit data sent from the collector 26 at the audit data source 18 to the parser 20 at the downstream process location, Virtual Records sent from the parser 20 at the audit data source 18 to the detector 32 at the downstream process location, or Virtual Records sent from the detector 32 at the audit data source 18 to the inserter 22 at the downstream process location.

Thus, this element 38 cited by the current Office Action fails to teach the recited template of claims 1, 14, and 37.

Further, col. 2, lines 45-55 of *Drake* cited by the current Office Action provide:

The system [of U.S. Pat. No. 5,557,742] uses processing system inputs, which include processing system audit trail records, system log file data, and system security state data information to detect and report processing system intrusions and misuses. A misuse selection mechanism allows the detection system to analyze the process inputs for a selected subset of misuses. The processing system inputs are then converted into states that are compared, through the misuse engine, to a predefined set of states and transitions until a selected misuse is detected. Once a misuse has been detected, an output mechanism generates a signal for use by a notification and storage mechanism. The detection system then generates a text-based output report for a user to view or store.

As can be seen, this further cited portion of *Drake* also fails to teach a template for defining an output format, as recited by claims 1, 14, and 37.

Accordingly, while the above-identified elements of independent claims 1, 14, and 37 recite a template for defining the format of an output, *Drake* simply fails to teach at least this claimed element. Accordingly, Applicant respectfully requests withdrawal of the rejections of independent claims 1, 14, and 37.

#### **B. Dependent Claims 10, 11, 13, and 15-18**

Dependent claims 10, 11, 13, and 15-18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by *Drake*. In view of the above, Applicant respectfully submits that independent claims 1 and 14 are not anticipated by *Drake* because *Drake* fails to teach every element of those independent claims. Further, each of dependent claims 10, 11, 13, and 15-18 depend either directly or indirectly from one of independent claims 1 and 14, and thus inherit all limitations of the respective independent claim from which they depend. It is respectfully submitted that dependent claims 10, 11, 13, and 15-18 are allowable not only because of their dependency from their respective independent claims for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective base claim from which they depend).

#### **IV. Rejections Under 35 U.S.C. § 103(a)**

Claims 2-9, 19-36, and 38-39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of *Sutton*. Also, claim 12 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Drake* in view of *Maloney*. Dependent claims 2-9, 12, 19-25, and 38-39 each depend either directly or indirectly from one of independent claims 1, 14, and 37, and thus inherit all limitations of the respective independent claim from which they depend. It is respectfully submitted that dependent claims 2-9, 12, 19-25, and 38-39 are allowable not only because of their dependency from their respective independent claims for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective base claim from which they depend).

Additionally, Applicant respectfully submits that independent claim 26 is not obvious under 35 U.S.C. § 103(a) over *Drake* in view of *Sutton*, as discussed further below. To establish a prima facie case of obviousness, three basic criteria must be met. See M.P.E.P. § 2143. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references must teach or suggest all the claim limitations. Without conceding any other criteria, Applicant respectfully asserts that the rejection does not satisfy the third criteria.

Independent claim 26 recites in part “accessing an audit transformation template that defines a desired format; and generating an output that includes at least a portion of said collected audit data, wherein said output comprises said desired format as defined by said audit transformation template” (emphasis added).

As described above, *Drake* fails to teach or suggest an audit transformation template that defines a desired format for generated output. *Sutton* also fails to teach or suggest this element. Accordingly, the applied combination of *Drake* and *Sutton* fails to teach or suggest at least the above elements of independent claim 26. As such, independent claim 26 is not obvious under 35 U.S.C. § 103(a) over *Drake* in view of *Sutton*. Therefore, Applicant respectfully requests that this rejection be withdrawn.

Also, dependent claims 27-36 each depend either directly or indirectly from independent claim 26, and thus inherit all limitations of independent claim 26. It is respectfully submitted that dependent claims 27-36 are allowable not only because of their dependency from independent claim 26 for the reasons discussed above, but also in view of their novel claim features.

**V. New Claims 40-54**

New claims 40-53 are presented herein. Claims 40-53 each depend either directly or indirectly from one of independent claims 1, 14, 26, and 37, and thus inherit all limitations of the respective independent claim from which they depend. As described above, independent claims 1, 14, 26, and 37 are believed to be of patentable merit. It is respectfully submitted that dependent claims 40-53 are allowable not only because of their dependency from their respective independent claims for the reasons discussed above, but also in view of their novel claim features (which both narrow the scope of the particular claims and compel a broader interpretation of the respective base claim from which they depend).

Additionally, new claim 54 is an independent claim that recites elements not taught or suggested by the references of record, and is therefore believed to be allowable over the references of record.

**VI. Conclusion**

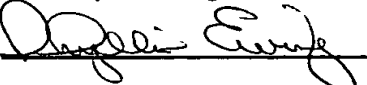
In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue.

Please charge any fee due to Deposit Account No. 08-2025, under Order No. 10013502-1 from which the undersigned is authorized to draw.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 482734960 US in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: August 6, 2004

Typed Name: Phyllis Ewing

Signature: 

Respectfully submitted,

By: 

Jody G. Bishop

Attorney/Agent for Applicant(s)

Reg. No. 44,034

Date: August 6, 2004

Telephone No. (214) 855-8007